DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

JUN 18 2003

MEMORANDUM FOR FRANK KIST
DIRECTOR
ENTERPRISE NETWORKS M:I:T

FROM: Charlene Wright Thomas
              Acting Privacy Advocate CL:PA

SUBJECT: Visionael
              Privacy Impact Assessment (PIA)

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment for the Visionael infrastructure application. Based on the information you provided, we do not have any privacy concerns that would preclude this system from operating. However, a revised PIA is required when considering any future upgrades or major modifications are made to the system.

We will forward a copy of the PIA to the Certification Program Office to be included in the Security Accreditation Package for formal acceptance for operation. The Office of Security Policy Support & Oversight, which has security oversight responsibility, may request information concerning the statements contained in the PIA to ascertain compliance with applicable requirements.

If you have any questions, please contact me at 202-927-5170 or you may contact Brian D. Townsend at 202-927-5162.

Attachment

Cc: Director, Certification Program Office M:S:A:C
      Director, Office of Security Policy Support & Oversight M:S:S
      Division Information Officer, MITS

Date   3/28/03

MEMORANDUM FOR CHARLENE W. THOMAS
                 ACTING PRIVACY ADVOCATE CL:PA

FROM: Frank Kist
                    Director, Enterprise Networks   M:I:EN

SUBJECT: Request for Privacy Impact Assessment (PIA) –
                    Visionael

Purpose of the System: The Visionael application, consisting of a database server, Web server, file server, and multiple logical application servers, is an enterprise-class network inventory software application that provides the capability to document and make available in a user-friendly interface an enterprise's telecommunications and call center network data. The Visionael application was purchased to provide PRIME a much more capable way of managing the discovered site infrastructure and network information gathered by the Infrastructure Discovery Teams (IDTs) during the Customer Communications 2001 (CC-2001) modernization project and has been transitioned to IRS Enterprise Networks Division. Visionael is currently being used to support the Large to Mid-Side business (LMSB) Virtual Private Network (VPN) deployments by capturing the baseline configuration of deployed LMSB VPN fixed sites.

Name of Request Contact:
        Name: Barbara A. Shammas
        Organization Name & Symbols: M:I:EN:P
        Mailing Address: 5000 Ellin Road, B4-350
                            Lanham, MD 20706
        Phone Number (with area code): (202) 283-5792

Name of Business System Owner:
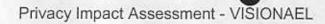   Name: Frank Kist
        Organization Name & Symbols: Enterprise Networks   M:I:EN
        Mailing Address: 5000 Ellin Road, B5-100
        Phone Number (with area code): (202) 283-7820

Requested Operational Date: 03/15/03

Category: (Reason PIA is required--enter "y" or "n" and applicable dates)
        New System?: ____X____
        Recertification? (if no change, enter date of last certification) _____
        Modification of existing system?: _____

Is this a National Standard Application (NSA)?: __NO____
Is this a Modernization Project or System? __NO____
If yes, the current milestone?: ____ (Enter 1-5; explain if combining milestones)

System of Record Number(s) (SORN) #: Treasury/IRS 34.037 IRS Audit Trial and Security Records System

Attachment: PIA

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:
 	
    A. Taxpayer
    B. Employee
    C. Audit Trail Information (including employee log-in info)
    D. Other (Describe)
	A. No taxpayer data.
	B. Name, Title, Organization, Email Address, Phone Number
	C. Visionael Audit Trail information is kept for changes to objects in the database. Login/logout files are managed by the operating system.
	D. Network inventory information including: name of device, location, IP address, subnet mask, default gateway, serial number

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.
 	
    A. IRS
    B. Taxpayer
    C. Employee
    D. Other Federal Agencies (List agency)
    E. State and Local Agencies (List agency)
    F. Other third party sources (Describe)
	A. Network inventory information including: name of device, location, IP address, subnet mask, default gateway, serial number
	B. No taxpayer data.
	C. Name, Title, Organization, Email Address, Phone Number
	D. No data from other Federal Agencies.
	E. No data from State and Local Agencies.
	F. No data from third party sources.

3. Is each data item required for the business purpose of the system? Explain.	Yes, to document IRS' network infrastructure.
4. How will each data item be verified for accuracy, timeliness, and completeness?	The Visionael System Administrator verifies the employee user registration before it is entered into the system. There is an automatic workflow approval process to ensure accuracy timeliness and completeness of network data.
5. Is there another source for the data? Explain how that source is or is not used.	No.

6. Generally, how will data be retrieved by the user?	The user will retrieve the data geographically or by network component. The data will not be retrieved by a personal identifier or other unique identifier. Individual users are limited to their own data using Visionael Studio software. Only System Administrators have access to all data in the database.
7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?	No, the data is not retrievable by a personal identifier.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?	System Administrators will have access to all data in the data base. Registered users are limited to their own data using Visionael Studio software.
9. How is access to the data by a user determined and by whom?	Access to the data is determined by the System Administrator based on a registers user's position and need to know. The System Administrator grants access and privileges to registered users using Form 5081. User access is terminated when it is no longer required.
10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared. If NO, continue to Question 12.	No.
11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?	N/A
12. Will other agencies provide, receive, or share data in any form with this system?	No.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?	Visionael is an active database that is automatically updated. The planned retention period for full backups is 6 months. At the end of 6 months, the backup tapes will be degaussed and destroyed per IRM 25.10.1.5.7.4.
14. Will this system use technology in a new way? If "YES" describe. If "NO" go to Question 15.	No.
15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.	No.
16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.	N/A because this is an infrastructure application.
17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.	No.
18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?	No.
19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?	No.